Remarks

Reconsideration of this Application is respectfully requested. Claims 24-31 are pending in the application, with claim 24 being the independent claim. Based on the above amendment and the following remarks, Applicants respectfully request that the Examiner reconsider all outstanding objections and rejections and that they be withdrawn.

Allowable Subject Matter

Applicant notes with appreciation the indication that claims 25-28 would be allowable if rewritten in independent form including all of the limitations of the base claim and any intervening claims.

Objection under 37 C.F.R. 1.75

Claim 31 was objected to under 37 C.F.R. §1.75(c), as being of improper dependent form for failing to further limit the subject matter of a previous claim. Applicant respectfully traverses this objection.

The RC4 stream cipher includes an algorithm to generate a random byte (key byte) and an algorithm to initialize the S-box via a shuffling operation. Amended claim 24 recites "wherein during a clock cycle in a key generation process the cryptographic core is configured to" perform a set of operations. Amended claim 31 recites "wherein the cryptographic core is further configured to shuffle the values stored in the memory addresses of the multi-ported memory during a clock cycle in an Sbox initiation process prior to the key generation process." Thus, claim 31 further limits independent 24 and is therefore a proper dependent claim. Reconsideration and withdrawal of the objection are therefore respectfully requested.

Rejections under 35 U.S.C. § 103

Matthews and Parker

Claims 24, 29, and 31 were rejected under 35 U.S.C. §103(a) as being unpatentable over Matthews, Jr., U.S. Patent No. 6,549,622 (Matthews) in view of Parker, et al, U.S. Publication No. 20020186839 (Parker). Applicant respectfully traverses this rejection.

The combination of Matthews and Parker does not teach or suggest each and every limitation of independent claim 24. The Office Action appears to equate the four stages of Applicant's recited pipeline to the clock cycles described in Matthews and Parker. Applicant respectfully disagrees with this understanding.

Matthews describes a key computation module 404 having a first dual port memory 604 and a second, redundant, dual port memory 606. (Matthews, FIG. 6). In Matthews, a dual port memory "supports a reduction in the number of cycle counts for performing the encryption or decryption algorithm from a 6 to 3 cycle core" and a pair of dual port memories "support[s] a reduction in the number of cycle counts for performing an encryption or decryption algorithm from a 6 to a 2 cycle core." (Matthews, col. 4, line 25 - col. 5, line 9). Matthews describes a set of operations performed in a series of clock cycles during an RC4 encryption or decryption process. (Matthews, col. 4, line 35 - col. 5, line 9). In Matthews, a byte of the key stream is not generated in each subsequent clock cycle after a set of initialization clock cycles. Instead, in Matthews, a portion of the key stream is generated after the completion of multiple clock cycles. For example, as shown in Table 4 of Matthews, a first portion of the key stream is generated in four clock cycles and a subsequent portion of the key stream is generated every two clock cycles thereafter.

Parker describes "a multiple-port memory 236 that stores the key and state array values." (Parker, para. [0026]). The cipher engine described in Parker "permits the implementation of the standard ARCFOUR algorithm in four clock cycles." (Parker, para. [0046]). Like Matthews, in Parker a byte of the key stream is not generated in each subsequent clock cycle after a set of initialization clock cycles. Instead, in Parker, a portion of the key stream is generated after the completion of multiple clock cycles. (Parker, ¶[0049])("Finally, x_cnt register 226 is incremented by one in preparation for the next iteration of the standard ARCFOUR algorithm.").

Thus, neither Matthews nor Parker include a multi-stage pipeline configured to generate a byte of key stream in each clock cycle after an initialization sequence. The combination of Matthews and Parker does not teach or suggest, at least:

> a cryptographic core having a four-stage pipeline, wherein during a clock cycle in a key generation process the cryptographic core is configured to:
>
> in a first stage, increment the value of a first memory address location,
>
> in a second stage, read data stored at a previous first memory address location and calculate a value of a second memory address location,
>
> in a third stage, read data stored at a previous second memory address location, calculate a value of a third memory address location, and write data stored at a previous first memory address location to the previous second memory address location, and
>
> in a fourth stage, read data stored at a previous third memory address location and write data stored at the previous second memory address location to a previous first memory address location,
>
> wherein after three initialization clock cycles, a byte of a key stream is generated in the fourth stage by the cryptographic core in each subsequent clock cycle.

as recited in amended independent claim 24. For at least these reasons, amended independent claim 24 is patentable over the combination of Matthews and Parker.

Claim 29 and 31 depend from claim 24. For at least these reasons, and further in view of their own features, claims 29 and 31 are also patentable over the combination of Matthews and Parker. Reconsideration and withdrawal of the rejection are therefore respectfully requested.

Matthews, Parker, and Batcher

Claim 30 was rejected under 35 U.S.C. §103(a) as being unpatentable over Matthews and Parker as applied to claim 29 and further in view of Batcher, U.S. Patent No. 6,873,707 (Batcher). Applicant respectfully traverses this rejection.

Claim 30 depends from independent claim 24. Batcher does not overcome all the deficiencies of Matthews and Parker relative to independent claim 24. For at least these reasons, and further in view of its own features, claim 30 is patentable over the combination of Matthews, Parker, and Batcher. Reconsideration and withdrawal of the rejection are therefore respectfully requested.

Double Patenting

Claims 24, 29, and 31 were also rejected on the ground of alleged nonstatutory double patenting over claims 9, 11, and 15 of Matthews in view of Parker. Applicant respectfully traverses this rejection.

A nonstatutory double patenting rejection is appropriate where the conflicting claims are not identical but at least one examined claim is not patentably distinct from the reference claim because the examined application claim is anticipated or would have been obvious over the reference claim. (MPEP § 804). As discussed above, amended independent claim 24 of the present application ("the examined independent claim") is not anticipated by or obvious over claims 9, 11, or 15 of Matthews ("the

reference claims") alone or in combination with Parker. For example, the reference claims do not teach or suggest at least:

> a cryptographic core having a four-stage pipeline, wherein during a clock cycle in a key generation process the cryptographic core is configured to:
>
> in a first stage, increment the value of a first memory address location,
>
> in a second stage, read data stored at a previous first memory address location and calculate a value of a second memory address location,
>
> in a third stage, read data stored at a previous second memory address location, calculate a value of a third memory address location, and write data stored at a previous first memory address location to the previous second memory address location, and
>
> in a fourth stage, read data stored at a previous third memory address location and write data stored at the previous second memory address location to a previous first memory address location,
>
> wherein after three initialization clock cycles, a byte of a key stream is generated in the fourth stage by the cryptographic core in each subsequent clock cycle.

as recited in the examined independent claim. Accordingly, reconsideration and withdrawal of the double patenting rejection are respectfully requested.

Conclusion

All of the stated grounds of objection and rejection have been properly traversed, accommodated, or rendered moot. Applicant therefore respectfully requests that the Examiner reconsider all presently outstanding objections and rejections and that they be withdrawn. Applicant believes that a full and complete reply has been made to the outstanding Office Action and, as such, the present application is in condition for allowance. If the Examiner believes, for any reason,

that personal communication will expedite prosecution of this application, the Examiner is invited to telephone the undersigned at the number provided.

Prompt and favorable consideration of this Reply is respectfully requested.

Respectfully submitted,

STERNE, KESSLER, GOLDSTEIN & FOX P.L.L.C.

Lori A. Gordon
Attorney for Applicant
Registration No. 50,633

Date: October 31, 2007

1100 New York Avenue, N.W.
Washington, D.C. 20005-3934
(202) 371-2600
742092_1.DOC